TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUS

OPINNÄYTETYÖRAPORTTI

TIETOTURVAOHJEISTUS

Case: Vapaa Valinta

Irene Sampakoski
Jenny Sihvo

Tietojenkäsittelyn koulutusohjelma
Marraskuu 2006
Työn ohjaaja: Petri Heliniemi

TAMPERE 2006

TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUS

Tekijä(t) Irene Sampakoski – Jenny Sihvo

Koulutusohjelma(t) Tietojenkäsittely

Tutkintotyön nimi Tietoturvaohjeistus case: Vapaa Valinta

Title in English Data security instructions case: Vapaa Valinta

Työn valmistumis-kuukausi ja -vuosi Marraskuu 2006

Työn ohjaaja Petri Heliniemi **Sivumäärä:** 44

TIIVISTELMÄ

Toimeksiantajanamme on Vapaa Valinta, joka on osa Tokmanni Oy:tä. Tokmanni on Suomen suurin halpakauppojen myymäläketju, jonka toiminta-alueena on koko Suomi. Koko konserniin kuuluu yhteensä 113 myymälää. Vapaa Valinta halusi tietoturvaohjeistuksen myymälöille ja varastolle. Yhteinen tietoturvaohjeistus soveltuu kaikkiin myymälöihin ja varastolle, koska toimintaperiaatteet ovat kaikilla samanlaiset. Heillä ei ole ollut resursseja itsellään tutkia tietoturvan nykytilaa ja tehdä sen perusteella tietoturvaohjeistusta.

Opinnäytetyömme tarkoituksena oli kartoittaa myymälöiden ja varaston tietoturvan nykytila ja tehdä tietoturvaohjeistus kartoituksen perusteella. Nykytilan selvitimme kyselylomakkeiden ja haastatteluiden avulla. Myymälöillä ja varastolla ei ole ollut ajantasalla olevia tietoturvaohjeita, joten opinnäytetyöstämme on hyötyä myymälä- ja varastohenkilökunnalle sekä Vapaa Valinnan atk-osastolle.

Tietoturvasta olemme saaneet tietoa aiemmin koulussa monilla kursseilla, esimerkiksi Tietoturvan perusteet –kurssilla. Aihetta on käsitelty kursseilla monista eri näkökulmista, eli meillä molemmilla oli jo perustiedot tietoturvallisuudesta. Syvensimme tietämystämme lähdekirjallisuuden avulla. Työssämme esittelemme yrityksen tietoturvaan liittyviä asioita.

Kyselylomakkeiden ja haastatteluiden avulla saimme selvitettyä hyvin tietoturvan nykytilan ja tehtyä yleisen tietoturvaohjeistuksen. Keräsimme haastatteluilla tietoa siitä, mistä henkilökunta haluaa lisätietoja. Jatkossa ohjeistusta tulee päivittää säännöllisesti ja tarkentaa tilanteen mukaan.

Avainsanat: tietoturva yrityksen tietoturva tietoturvaohjeet

TAMPERE
POLYTECNIC

Author(s)	Irene Sampakoski – Jenny Sihvo
Degree Programme(s)	Business Information Systems
Title	Data security instructions case: Vapaa Valinta
Month and year	November 2006
Supervisor	Petri Heliniemi

Pages: 44

ABSTRACT

Our client is Vapaa Valinta, which is a part of Tokmanni Ltd. Tokmanni is biggest chain of discount stores in Finland, and it area of operation is whole Finland. To Tokmanni consolidated corporation belongs altogether 133 stores. Vapaa Valinta needed data security instructions to stores and to warehouse. Common data security instructions lends to every store and to warehouse, because they all act same way. Vapaa Valinta did not have resource itself at the moment to search through its present state of data security.

Our thesis purpose was to survey present state of data security in stores and in warehouse and do data security instructions. Present state we shorted out with help of questionnaires and interviews. Stores and warehouse did not have data security instructions, so they and ADP department benefit from our thesis.

We have learned about data security in school at many courses. This subject is handled on courses from different point of views, we both had already basic information about data security. We deepened our knowledge with help of source books. In our thesis we introduce things that relate to company data security.

By using questionnaires and making interviews, we found out well the situation of data security,
and make universal data security instructions. With interviews we collected information about, where from employees want information. In future the instructions should be updated regularly and define depending about situation.

Keywords: data security companies data security data security instructions

Sisällysluettelo

1 Johdanto

1.1 Vapaa Valinta

Opinnäytetyön toimeksiantaja on Vapaa Valinta. Yrityksen toiminta alkoi vuonna 1974 Nokian Tekstiili -nimisenä liikeyrityksenä. Nimestä muodostui lyhenne Notex Oy, myöhemmin Notex-Yhtiöt Oy. Markkinointinimi Vapaa Valinta otettiin käyttöön vuonna 1979. Nykyään Vapaa Valinta myymälät ovat osa Tokmanni Oy:tä. Tällä hetkellä myymälöitä on 36 ympäri Länsi-Suomea sekä Vapaa Valintoihin lukeutuva Milleri. Vapaa Valinta ja Milleri työllistää tällä hetkellä yli 300 työntekijää.

Marraskuusta 2004 Vapaa Valinnasta tuli osa Tokmanni Oy:tä ja näin myös osa suurempaa myymäläketjua, kun Notex-Yhtiöt Oy myi Vapaa Valinta-myymälät Tokmanni Oy:lle. Tällä hetkellä Tokmanni Oy:n kuuluu Tokmanni-myymälät, Tarjoustalo, Vapaa Valinta, Maxi-Makasiini, Maxi-Kodintukku, säästötalo Robin Hood ja Säästökuoppa. Tokmanni Oy on muutaman vuoden aikana laajentunut Suomen suurimmaksi halpakauppojen myymäläketjuksi, jonka toiminta-alueena on koko Suomi. Tokmanni-nimellä toimii 28 myymälää Itä-Suomessa, Etelä-Suomen 24 myymälää ovat Tarjoustaloja. Pirkanmaalla, Lounais- ja Länsi-Suomessa on 36 Vapaa Valintaa, Oulun seudulla ja Pohjois-Suomessa on neljä Säästökuoppaa. Kaakkois-Suomessa ja Kymenlaaksossa on kymmenen Robin Hoodia, Kainuussa ja Ylä-Savossa kymmenen Maxi-Makasiinia ja Maxi-Kodintukkua. Koko konserniin kuuluu yhteensä 113 myymälää.

Aiemmin Vapaa Valinta -myymälöillä, varastolla, eikä myöskään Millerillä ole ollut tietoturvaohjeistusta tai opasta. Yhteinen tietoturvaohjeistus soveltuu hyvin kaikkiin Vapaa Valintoihin ja Milleriin, koska toimintaperiaatteet ovat kaikilla samanlaiset.

1.2 Taustaa opinnäytetyöstä

Vapaa Valinta halusi kartoittaa tietoturvansa nykytilan ja tehdä tietoturvaohjeistuksen myymälöille ja varastolle sekä tietoa myymälöiden tarvitsemista erillisistä ohjeistuksista. Toimeksiantajallamme ei ole ollut resursseja itsellään tutkia tietoturvan nykytilaa tarkemmin. Näin ollen opinnäytetyömme tavoitteeksi tuli perehtyä tietoturvaan syvemmin ja kartoittaa myymälöiden ja varaston tietoturvan nykytila kyselylomakkeiden avulla ja niiden pohjalta tehdä yleispätevä tietoturvaohjeistus Vapaa Valinnalle. Teimme kyselylomakkeen, jonka avulla selvitimme tämänhetkisen tilanteen. Kyselylomakkeen tekeminen oli haastavaa, koska etukäteen mietittäviä asioita oli paljon. Kävimme henkilökohtaisesti neljässä eri myymälässä ja varastolla haastattelemassa eri työtehtä-

vissä olevia henkilöitä. Haastatteluiden ja kyselylomakkeiden avulla saimme selville, missä kohdissa heidän toimintansa tarvitsee päivitystä ja korjausta. Teimme ohjeet nimenomaan myymälöille ja varastolle. Niistä oli tarkoitus tehdä kattavat yleisohjeet, jotta ne käyvät sekä myymälöihin että varastolle. Niillä ei ollut ajantasalla olevia tietoturvaohjeita, joten työstämme on hyötyä kaikille myymälöille ja myös Vapaa Valinnan atk-osastolle. Ohjeistus on myös tukena uuden työntekijän perehdyttämisessä. Atk-osaston ei tarvitse itse tehdä kyselyä ja nykytilan kartoitusta, joten se voi aloittaa suoraan tarvittavat toimenpiteet tietoturvan lisäämiseksi. Parannustoimet tullaan tekemään haastatteluiden ja kyselyjen analysoinnissa ilmenevien puutteiden perusteella. Myymälöissä ja varastolla tietoturva tulee toivottavasti lisääntymään työmme ansiosta ja henkilökunta tulee ylipäätään tietoisemmiksi tietoturvaan liittyvistä hyödyistä ja riskeistä.

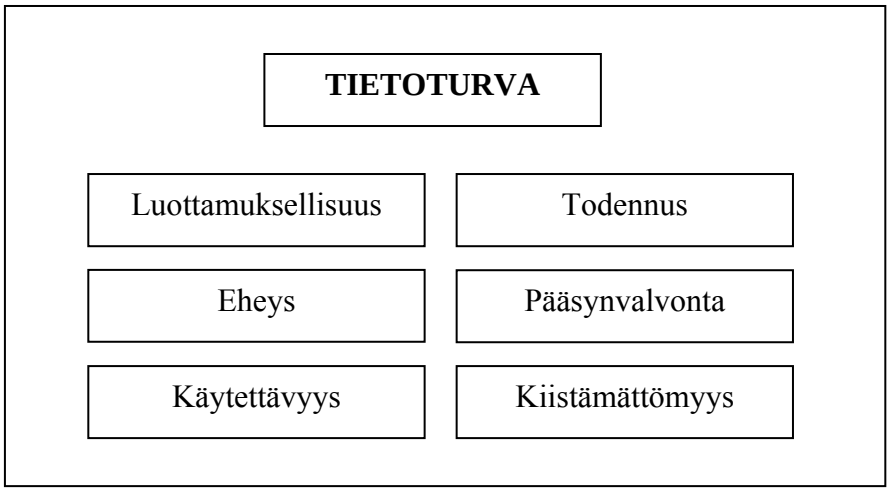
Kirjallisuutta etsiessämme huomasimme, että tietoturvaohjeistukseen liittyvää ajankohtaista kirjallisuutta löytyi melko vähän. Petteri Järvisen vuoden 2002 kirjassa oli hyvin perustietoa tietoturvasta ja erityisesti tietoa yrityksen tietoturvasta. Tietoturva-asiat muuttuvat jatkuvasti, siksi Petteri Järvisen uusin kirja oli luotettavin kirjalähteistä. Siinä oli hyvin ajankohtaista tietoa. Internetistä ja lehtiartikkeleista löytyi myös paljon ajankohtaista tietoa. Päivitimme myös kirjoista löytynyttä tietoa Internetistä löytyneen tiedon avulla. Kirjoissa oli mielestämme perustiedot kattavasti, mutta uusimmat teknologiat ja ratkaisut löytyivät Internetistä ja alan lehdistä.

2 Yleistä tietoturvasta

Tässä kappaleessa esitellään yleisesti tietoturva-asioita. Tietoturva on tiedon luotettavuudelle asetettuja kriteereitä ja se perustuu lainsäädäntöön. Siitä huolehtiminen kuuluu kaikille. Tietoturvallisuus on paljon muutakin kuin virustorjuntaa, salasanoja tai viestien salakirjoittamista. Sitä tarvitaan tietojenkäsittelyn kaikilla tasoilla laitteistoista ihmisiin ja yhteisöihin asti ja kaikilla sovellusalueilla, joissa käsiteltävillä, siirrettävillä tai talletettavilla tiedoilla on jollekulle jotain arvoa.

Tietoturva on perusta, jolle tärkeiden ja luottamuksellisten tietojen käsittely rakentuu. Yritysten näkökulmasta tärkeitä tietoja ovat mm. henkilöstöön, palkkoihin, tuotteisiin tai myyntilukuihin liittyvät tiedot. Niiden suojaaminen on yritystoiminnan jatkumisen edellytys. (Järvinen 2002: 21.)

Kuvassa 1 esitetään tietoturvan keskeisiä käsitteitä, joita ovat luottamuksellisuus, eheys, käytettävyys, todentaminen, pääsynvalvonta ja kiistämättömyys. Luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat vain tietojen käyttöön oikeutettujen käytössä ja muut eivät pääse niihin käsiksi. Eheydellä tarkoitetaan, että tiedot ja järjestelmät ovat luotettavia, oikeita ja ajantasaisia, eivätkä tiedot pysty hallitsemattomasti muuttumaan missään tilanteessa. Käytettävyys tarkoittaa, että järjestelmien tiedot ja palvelut ovat niihin oikeutettujen käytettävissä etukäteen määritellyssä vasteajassa, eivätkä tiedot ole tuhottavissa. Todentaminen tarkoittaa osapuolten luotettavaa tunnistamista. Pääsynvalvonnalla tarkoitetaan, että käyttäjien pääsyä koneessa olevaan tietoon rajoitetaan ja valvotaan. Pääsynvalvonnalla tarkistetaan, onko osapuolella oikeus palvelun ja tiedon käyttöön, jolloin vain todennetut henkilöt pääsevät käyttämään tietoja. Kiistämättömyys tarkoittaa tapahtuneen todentamista jälkeenpäin, tällä varmistetaan, ettei toinen osapuoli voi kieltää toimintaansa jälkeenpäin. (Valtiovarainministeriö 2003)



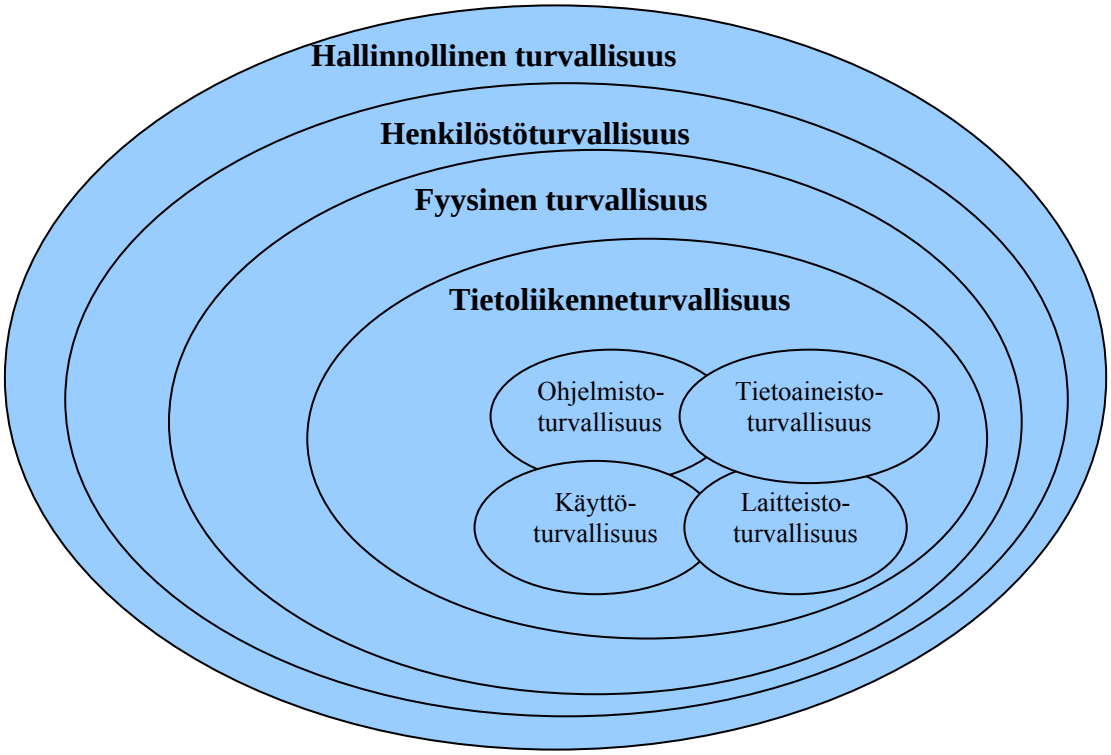
Kuva1 Tietoturvan kuusi keskeistä käsitettä

Tietoturva on osa yrityksen liiketoimintaa. Yritykselle tärkeän tiedon turvaaminen on yksi menestymisen ehto. Tieto on yrityksen liiketoiminnalle tärkeää silloin, kun sen puuttuminen, virheellisyys tai paljastuminen tuottaisi taloudellisia tai muita vahinkoja. Tietoturvassa ei ole kyse vain tekniikasta, vaan ihmisten työskentelytavoista. Kaikkien tulee tietää, kuinka tietoturvasta voidaan huolehtia. On myös tietoja, joiden turvaamiseen yrityksellä on lainsäädännön velvoite.

Ohjeistukset ja pelisäännöt ovat yrityksen tietoturvan perusta, joista Järvinen (2002: 115) kirjoittaa seuraavasti. ”*Toimintaohjeet määrittelevät kirjaimellisesti, miten varmuuskopiointi, ohjelmien päivittäminen tai uuden käyttäjätunnuksen luominen (ja varsinkin sen poistaminen, kun henkilö lopettaa) tehdään. Ohjeen lisäksi jokaiselle tehtävälle on nimitettävä vastuuhenkilö ja tämän varahenkilö, joka viimekädessä vastaa asian suorittamisesta ja ohjeiden säännöllisestä päivittämisestä. Toimintaohjeet menettävät merkityksensä ja uskottavuutensa, jos ne eivät pysy ajan tasalla, vaan kuvaavat parin vuoden takaista tilannetta. Toimintaympäristön jatkuva muuttuminen pakottaa uusimaan myös ohjeita säännöllisesti.”* Mielestämme tällaisten ohjeiden olemassaolo yrityksessä on tärkeää ja olemme samaa mieltä Järvisen kanssa ohjeiden päivittämisestä.

Yrityksen liiketoiminnan kannalta tärkeä tieto ei ole vain sähköisessä muodossa, vaan kaikki tieto papereissa ja puhuttunakin on tärkeää. Hyvä tietoturva ei välttämättä vaadi suuria investointeja, vaan pienikin panostus voi hyödyttää liiketoimintaa. Tietoturvan pyrkimyksenä on kattaa kaikki se, mikä liittyy tietojen saatavuuteen, oikeellisuuteen sekä tietojen luottamuksellisuuden säilyttämiseen käsittelyn, säilytyksen ja tiedonsiirron aikana. Suomen valtionhallinnon virallinen määritelmä tietoturvalle, niin kutsuttu sipulimalli, jakaa tietoturvan kahdeksaan osa-alueeseen. Neljä ulointa kerrosta ovat: hallinnollinen tietoturva, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus. Näiden neljän kerroksen suojaamana ovat sisimpänä: ohjelmistoturvallisuus, tietoaineistoturvallisuus, käyttöturvallisuus, laitteistoturvallisuus. Kuva 2.

Hallinnollinen tietoturva pitää sisällään organisaation tietoturvaan tekemät linjaukset ja yleisen tietoturvan toimintapolitiikan. Henkilöstöturvallisuus koskee työntekijöitä, heidän ohjeistusta ja koulutusta. Fyysinen turvallisuus käsittää toimitilojen fyysisen suojauksen. Tietoliikenteen turvallisuus takaa tietoliikenteen jatkuvuuden, siirrettävän tiedon salaamisen ja eheyden varmistamisen. Laitteistoturvallisuus käsittää tietokoneiden ja verkon toimivuuden. Ohjelmistoturvallisuus käsittää käytettyjen ohjelmistojen suojaamisen. Tietoaineistoturvallisuus pitää sisällään levyjen, levykkeiden, nauhojen ja tulosteiden turvallisen käsittelyn niin, etteivät luottamukselliset tiedot joudu vääriin käsiin. Käyttöturvallisuus on tietokoneiden ja verkon aktiivilaitteiden päivittäiseen käyttöön liittyvien asioiden turvaamista. (Järvinen 2002: 112)



Kuva2 Suomen valtionhallinnon virallinen määritelmä tietoturvalle (nk. sipulimalli)

Kotilainen (2006) on kirjoittanut mielenkiintoisen artikkelin Turvallisuus-lehteen yrityksen kokonaistietoturvasta, jossa hän haastattelee tietoturvakonsultti Otto Peltomaata. *”Lähes poikkeuksetta yritysten tietohallinto on investoinut tekniikkaan: palomuureihin, virustorjuntaan, varmistusjärjestelmiin ja hyökkäysten estoon. Se puoli on kenties parhaiten kunnossa. Sen sijaan useista organisaatioissa puuttuu tietoturvallisuuteen liittyvä johtaminen ja koko tietoturvapolitiikka. Tietoturvallisuudesta vastaavat henkilöt kyllä tietävät yrityksen turvallisuuteen liittyvät määräykset ja käytännöt, mutta niiden viestittäminen muulle henkilökunnalle on jäänyt tekemättä*.” Artikkelissa tuli esiin niitä asioita, joita tutkimuksessamme huomasimme. Atk-osasto on valveutunut ja tietää asioista, mutta muulla henkilökunnalla ei ole mielestämme tarpeeksi tietämystä asioista.

2.1 Päivittäminen

Järvinen (2006) kirjoittaa uusimmassa kirjassaan paljon päivittämisestä. Se on noussut tietoturvassa yhdeksi tärkeimmistä osa-alueista. Tämän päivän käyttöjärjestelmiä päivitetään niin useasti, että joillakin yrityksillä saattaa olla vaikeuksia pysyä tahdissa mukana.

Kaikkien käyttöjärjestelmien turvallisuus perustuu nykyisin päivityksiin. Säännöllinen päivittäminen on tietoturvan ensimmäinen edellytys. Palomuuri-

en ja viruksentorjuntaohjelmien päivittäminen on myös erittäin tärkeää. Päivitetyt versiot pystyvät torjumaan uusimmatkin virukset.

Päivittämisestä onkin tullut yhtä arkista rutiinia kuin siivouksesta. Vähintään kerran viikossa jokin ohjelma tai laite kaipaa päivittämistä, eikä kyse ole pelkistä tietokoneista ohjelmineen, vaan päivityksiä tarvitsevat niin matkapuhelimet, digikamerat, digiboksit, kuin monet muutkin kodin elektroniikkalaitteet.

Päivittäminen on tarpeen, koska laitteet tuodaan myyntiin keskeneräisinä. Kiireen vuoksi niihin jää virheitä, joita joudutaan paikkailemaan jälkikäteen. Joskus harvoin päivittäminen tuo myös uusia ominaisuuksia, esimerkiksi tuen jollekin uudelle protokollalle tai tekniikalle, jota ei vielä tuotteen valmistuessa ollut olemassa.

Tällainen päivittäminen pidentää tuotteen käyttöikää ja on siksi ns. huonoa bisnestä. Valmistajan kannalta on parempi, että asiakas saadaan päivittämisen sijaan ostamaan kokonaan uusi laite. Valmistajalla onkin tapana lopettaa ennen pitkää päivitysten julkaiseminen. Vaikka tuotteesta vielä löytyisi virheitä, niitä ei enää korjata. Päivitysten loppuminen viestittää käyttäjälle, että tämän olisi aika ostaa uusi laite. (Järvinen 2006: 15)

2.2 Palomuurit

Palomuurilla tarkoitetaan järjestelmää, ohjelmistoa tai laitteistoa, jolla yrityksen tietoverkkoja voidaan suojata tietoturvauhkia vastaan. Virustentorjuntaohjelma ei estä koneelle tulevia murtoyrityksiä. Tietomurtojen ja verkkohyökkäysten estämiseen tarvitaan palomuuri.

Aluksi palomuurit olivat hyvin tehokkaita suojaamaan yritystä ulkopuolelta tulevia hyökkäyksiä vastaan. Samalla voitiin rajoittaa myös yrityksestä ulospäin lähtevää liikennettä ja näin estää ei-toivottujen viihteellisten nettipalvelujen käyttö. Rajoitusten asentaminen oli helppoa IP-osoitteiden ja porttinumeroiden perusteella. (Järvinen 2006: 105)

Tänään tilanne on muuttunut. Palomuuri ei enää riitä suojaamaan yritystä, koska palomuurin ohi on muita reittejä. Oma henkilökunta ja vieraat tuovat yritykseen kannettavia tietokoneita, jotka liitetään yrityksen sisäverkkoon. Silloin koneissa mahdollisesti olevat haittaohjelmat pääsevät leviämään suoraan lähiverkkoon. Yrityksen tiloissa, esimerkiksi neuvotteluhuoneissa, olevan WLAN-tukiasemat saattavat päästää liikennettä sekä ulos että sisään palomuurin ohi. (Järvinen 2006:105)

Palomuuri on kuitenkin vielä tärkeässä asemassa ja monesti tärkeämpi kuin viruksentorjuntaohjelma. Palomuurista on suojaa sellaisissakin tilanteissa joihin omalla toiminnallaan ei pysty vaikuttamaan, kun taas virustorjunnassa käyttäjän toiminnalla on suuri merkitys. Tässäkin päivittäminen on tärkeässä roolis-

sa. Virukset voi välttää jos selain, käyttöjärjestelmä ja sähköpostijärjestelmä ovat ajantasalla, eikä avaa tiedostoliitteitä.

2.3 Haittaohjelmat

Sana haittaohjelma viittaa kaikkiin niihin ohjelmiin, jotka asentuvat koneelle salaa tai lupaa kysymättä ja tuottavat käyttäjälle haittaa. Vielä 1990-luvulla tähän kuuluivat vain virukset ja muutama harvinainen troijalainen. Mutta nopeiden verkkoyhteyksien myötä haittaohjelmien määrä ja uhkapotentiaali ovat nousseet uudelle tasolle. (Järvinen 2006: 78)

Haittaohjelmilla tarkoitetaan ihmisen tarkoituksellisesti tekemiä vahingollisia tietokoneohjelmia. Haittaohjelmista tyypillisimpiä ovat roskapostit eli virukset, madot ja troijalaiset. Yleisesti haittaohjelmalla tarkoitetaan sellaista ohjelmaa, jonka tarkoituksena on aiheuttaa tietojärjestelmissä ei-toivottuja tapahtumia. Myös sellaisia ohjelmia, jotka aiheuttavat tahattomasti haittaa tietojärjestelmille kutsutaan toisinaan haittaohjelmiksi. Haittaohjelmien kirjo on kasvanut valtavasti, niitä ovat muun muassa verkkomadot, virukset, bottiverkot, näppäimistökaapparit, modeemikaapparit, valeturvaohjelma, huijausviestit sekä vakoiluja mainosohjelmat. Useimmiten esille tulleita ovat virukset ja verkkomadot.

Virukset ovat pieniä tietokoneohjelmia, jotka hankaloittavat tai estävät muiden ohjelmien toimintaa tietokoneessa. Ne voivat aiheuttaa sen, että ohjelmat eivät toimi normaalisti tai niiden toiminta on huomattavasti hidastunut, jolloin tietokoneella ei voi työskennellä. Virus voi estää koko tietokoneen toiminnan. Virukset voivat myös tuhota tiedostoja tai lähettää koneeseen tallennettuja tietoja salaa eteenpäin. Tietokonevirus voi tuhota kaikki koneeseen tallennetut tiedostot ja ohjelmat.

Uusia haittaohjelmia suunnitellaan koko ajan. Haittaohjelmia ovat esimerkiksi virukset, madot ja troijalaiset. Madot ovat tietokoneohjelmia, jotka osaavat monistaa itseään ja levitä automaattisesti esimerkiksi sähköpostin välityksellä. Troijalaiset eli Troijan hevoset ovat nimensä mukaisesti ohjelmia, jotka sisältävät piilotettuja ohjelmoituja toimintoja. Troijan hevosen avulla hakkeri saattaa päästä käyttämään tietokonetta ulkopuolelta. Verkkomadot ovat ohjelmia, jotka leviävät automaattisesti verkkoyhteyksien yli, eivätkä ne tarvitse toimintaansa varsinaista isäntäohjelmaa. Madot hyödyntävät kuitenkin usein tartuttamaansa järjestelmää, esimerkiksi etsimällä järjestelmästä sähköpostiosoitteita ja lähettämällä itsensä kaikkiin näihin osoitteisiin.

2.4 Käyttäjätunnukset ja salasanat

Käyttäjätunnus on sisään kirjauksen yhteydessä käyttäjän ilmoittama, hänet yksilöivä, tunniste. Kun kirjaudutaan sisään johonkin palveluun, vaikka lukemaan sähköposteja tai omalle koneelle, palvelu tunnistaa käyttäjän hänen määrittämänsä tunnuksen perusteella. Tietojärjestelmien käyttöön tarvitaan aina

käyttöoikeus. Käyttöoikeus on henkilökohtainen ja se on usein yhdistetty käyttäjän henkilöllisyyteen ja työtehtävään. Käyttäjätunnusta ja salasanaa tulee käsitellä samalla tavalla kuin esimerkiksi pankkikorttia ja sen tunnuslukua.

Käyttäjätunnus voidaan muokata esimerkiksi nimen alkukirjaimista. Käyttäjätunnus on looginen ja julkinen. Käyttäjätunnuksen parina kirjautumisessa on salasana, joka on aina salainen.

Salasana on vain käyttäjän tiedossa oleva merkkijono, jonka avulla tietojärjestelmä voi todentaa käyttäjän tunnistuksen. Tällä varmistetaan, että käyttäjä on oikea, kun hän on antanut oikean käyttäjätunnuksen ja salasanan, voidaan asiasta olla varmoja. Tärkeä kohta määritelmässä on se, että salasana on vain käyttäjän tiedossa. Sitä ei saa kertoa kenellekään, eikä kirjoittaa muistiin. Käyttäjätunnus ja salasana tulee pitää erillään. Vaikka joku tietää käyttäjätunnuksesi, ei hän voi käyttää palveluita ilman salasanaasi.

2.5 Varmuuskopiointi

Varmuuskopioinnilla tarkoitetaan tiedon tallentamista useaan paikkaan sen sijaan, että se olisi tallennettuna vain yhdelle tallennusvälineelle. Näin tiedon saanti varmistetaan, jos jostain syystä alkuperäinen tallenne häviää tai tuhoutuu. Tiedon katoamisen tai vahingoittumisen taloudelliset seuraukset voivat olla yritykselle vakavia. Tarvittavista tiedostoista onkin syytä ottaa varmuuskopiot. Jos tiedot katoavat tai vaurioituvat, varmuuskopiot säästävät sekä kustannuksia että työaikaa.

Tiedostot voivat tuhoutua monesta syystä. Tiedostoja voi poistaa vahingossa konetta käytettäessä, tietokoneen kovalevy, levyke tai muu tallennusväline voi rikkoutua tai siihen tulla toimintavika. Näin ollen sille tallennettu aineisto saattaa tuhoutua tai niitä ei voi enää käyttää. Tietokoneen fyysinen rikkoutuminen siten, ettei tietoja voida enää pelastaa, ei ole mitenkään harvinaista. On syytä ottaa myös huomioon, että tiedostoja ja laitteita voi kadota ja niitä voidaan jopa varastaa.

Tietokonevirukset ja muut haittaohjelmat voivat myös aiheuttaa tiedostojen katoamisen. Varmuuskopiointi onkin olennainen osa tietoturvaa. Varmuuskopiointi on syytä tehdä mahdollisimman usein, jotta aineisto säilyminen varmistetaan. Varmuuskopioinnista olisikin syytä tehdä säännöllistä toimintaa.

3 Hyvä tietoturvaohjeistus

Tässä kappaleessa käsitellään hyvän tietoturvaohjeistuksen tarpeellisuutta yrityksessä. Sateenvarjona toimivan tietoturvapolitiikan alle tarvitaan yleisiä pelisääntöjä, yksityiskohtaisia toimintaohjeita, koulutusta ja poikkeustilanteisiin varautumista. On esimerkiksi mahdollista, että kaivinkone katkaisee sähkö- tai tietoverkkoyhteydet. Ellei varajärjestelyjä ole, yritys häviää Internetin maailmankartalta ja asiakkaiden ulottuvilta. (Järvinen 2002: 115)

Juhani Paavilainen (2004) on luetellut myös tietoturvamateriaalissaan, mitä ohjeita organisaatiossa tulisi olla. Ohjeita tulisi olla käyttäjätunnuksista ja salasanoista, yksityisyyden suojasta ja sähköpostinkäytöstä. Yrityksellä tulisi olla myös normaalit käyttötoimenpideohjeet, ylläpito-ohjeet, ohjeet poikkeustilanteita, tietoaineiston luokittelua, vaitiolosopimuksia ja salassapitosopimuksia varten sekä toipumisohjeet.

Tietoturvaopas.fi (2006) sivustolla kerrotaan tietoturvaohjeista. *”Tietoturvaohjeiden tavoitteena on estää ongelmien syntyminen. Ohjeet tarvitaan mm. yrityksen tiedon käsittelyyn, Internetin ja sähköpostin käyttöön sekä laitteiden ja järjestelmien käyttöön. Ohjeet on löydyttävä myös ongelmatilanteiden ja poikkeusolosuhteiden varalle. Miten yrityksessäsi on varauduttu esim. sähkökatkoon tai virustorjunnan pettämiseen?”*

Kun ohjeita viedään käytäntöön, ovat selkeästi määritellyt vastuut olennaisia. Henkilöstöllä tulee olla tiedossa, mistä asioista kukin huolehtii. Paula Koskivirta (2006) kirjoittaa artikkelissaan, että ”*vain pieni osa tietoturvallisuudesta hoidetaan tekniikan avulla, ja se kannattaa muistaa aina. Suurin osa tietoturvallisuudesta hoidetaan henkilöstön tietoturvallisen käyttäytymisen avulla. Siksi on tärkeä motivoida ja kouluttaa henkilöstö käyttäytymään tietoturvallisesti*.”

Turvaa lisäävien pelisääntöjen noudattaminen helpottuu, kun työntekijät ymmärtävät, miksi rajoituksia asetetaan ja miten heidän oma etunsa – jopa työpaikkansa – voi olla vaarassa, jos tietoturva pettää. Työntekijöiden pitäisi hahmottaa oma asemansa osana yritystä, sen julkista kuvaa ja osuutensa koko laajassa tietoturvan käsitteessä. (Järvinen 2002: 111)

3.1 Esimerkkikysymyksiä tieturvaohjeistukseen

Tietoturvaopas.fi (2006) sivustolla on lueteltu kysymyksiä, joita pohtimalla ja selvittämällä niihin vastauksia, saa hyvän rungon tietoturvaohjeistusta varten. Emme löytäneet paljon ohjeita hyvän tietoturvaohjeistuksen tekemiseen, mutta näistä kysymyksistä saimme apua. Otamme tässä kappaleessa esille Tietoturvaoppaan kysymyksiä.

Toimitiloihin kulkeminen
– Määritellään normaalit ja poikkeusreitit yrityksen tiloihin.
– Mitä reittejä käytetään hätätilanteessa?
– Kuka huolehtii kulkuluvista?

Yleiset ohjeet yrityksen tiloissa toiminnan suhteen
– Jos rakennuksessa tai samoissa tiloissa toimii useita yrityksiä, miten asia on tietoturvan suhteen huomioitu?
– Onko olemassa yhteisiä tiloja, joita käyttää useampi yritys? Vaikuttaako tämä esim. keskusteluihin asiakasprojekteihin liittyvistä asioista. Miten asiasta on annettu ohjeet henkilöstölle?

Verkon salasanat
– Kauanko salasanat ovat kerrallaan voimassa?
– Onko salasanan sisältöä ohjeistettu?
– Miten toimitaan, jos salasana unohtuu?
– Miten nopeasti salasana vanhenee?

Virustorjunta
– Mikä virustorjuntaohjelmisto on käytössä ja miten sen päivittämisestä on huolehdittu?

Sähköposti
– Miten salauksen käyttö sähköpostiviestien yhteydessä on ohjeistettu?
– Onko sähköpostiviestien liitteiden avaaminen ohjeistettu.

Verkosta imuroitujen ohjelmien asentaminen
– Mitä ohjelmia saa Internetistä asentaa työkoneille?

Varmuuskopiot
– Kuka huolehtii varmuuskopioinnista?
– Miten palvelinten varmuuskopioinnista on huolehdittu?

Tulosteet
– Onko tulostinten käyttö ohjeistettu?

Luottamuksellinen materiaali
– Luottamuksellista materiaalia sisältävää materiaalia ei tule heittää tavalliseen roskakoriin, vaan erilliseen lukittuun astiaan, josta ne hävitetään turvallisesti.

Työaseman ja kannettavan tietokoneen käyttö
– Kun omalta työasemalta poistutaan, tulee kone lukita (esim. painamalla kerran ctrl - alt - del). Näin näytöllä olevat tiedot pysyvät satunnaisilta ohikulkijoilta piilossa. Jos omalta työasemalta jaetaan tiedostoja muiden käyttöön tulee tarkastaa, kenelle pääsy tiedostoihin annetaan. Milloinkaan koko levyasemaa ei tule jakaa "juuresta", koska tällöin kaikki ko. levyn tiedot ovat jaossa.

– Oltaessa poissa toimistolta, kannettavaa konetta ei tule jättää näkyville autoon tai muuten lojumaan huolettomasti.
– Mikäli työhön liittyviä tiedostoja käsitellään kotikoneella, tulee huolehtia siitä, että ko. koneen palomuuri ja virustorjunta on ajan tasalla.

Demotilaisuudet
– Esittelytilaisuuksissa tarvittavat tiedostot tulee tallentaa koneelle tai varmistaa verkon yli niille pääsy ennen tilaisuuden alkamista. Mikäli tiedostoja haetaan yrityksen intranetistä palaverin aikana, tämä tulee tapahtua koneen oman näytön, ei videotykin näytön kautta. Palaverin jälkeen neuvotteluhuoneesta tulee siivota pöydille, tauluihin tai muualle jääneet muistiinpanot.

Internetin käyttö
– Miten netin käyttöä työssä ja työaikana on ohjeistettu? Onko netti vapaasti käytettävissä? Onko "epäilyttäviä" sivustoja määritelty?

Vieraat
– Miten vieraiden vastaanotto tapahtuu? Miten tietoturva on huomioitu neuvotteluhuoneen sijainnin suhteen. Pääsevätkö vierailijat tuotantotiloihin?

Alihankkijat ja freelancerit
– Projekteissa käytettävien alihankkijoiden ja freelancereiden kanssa tulee tehdä tarvittavat salassapitosopimukset ennen työn alkamista.

Edellä olevassa tietoturvaohjeistuksen kysymyksissä on huomioitu kattavasti useita tietoturvan osa-alueita. Tässä olisi mielestämme voitu vielä lisäksi pohtia henkilöstöturvallisuuteen liittyviä kysymyksiä tarkemmin. Ohjeissa ei ollut käsitelty esim. henkilöstön koulutusta tai motivaation ylläpitämistä, jotka ovat mielestämme erittäin tärkeitä asioita tietoturvallisuuden ylläpitämiseksi. Kysymykset ovat yleisiä, joten ne eivät täysin huomioi erilaisia toimialoja. Näin ollen mietimme Vapaa Valinnan ohjeistusta tehdessämme kaupanalalle sopivia kysymyksiä ja seikkoja.

4 Työmenetelmät

4.1 Yleistä kyselylomaketutkimuksesta

Kyselylomaketutkimuksessa vastaajat täyttävät heille annetun kyselylomakkeen. Tieto kerätään analysoimalla lomakkeita. Tämän vuoksi kysymykset tulee miettiä huolellisesti, koska niistä riippuu tutkimuksen onnistuminen. Eniten virheitä tutkimustuloksiin aiheuttavat kysymysten muodot. Ongelmana on, että vastaaja ei ajattele samalla tavalla kuin tutkija, tällöin tulokset voivat vääristyä. Kysymysten tulee olla tämän vuoksi yksiselitteisiä. Ennen kuin kysymyksiä lähdetään tekemään, tulee tavoitteiden ja tutkimusongelman olla selvillä.

Kyselytutkimuksen etuna pidetään yleensä sitä, että niiden avulla voidaan kerätä laaja tutkimusaineisto; tutkimukseen voidaan saada paljon henkilöitä ja voidaan myös kysyä monia asioita. Kyselymenetelmä on tehokas, koska se säästää tutkijan aikaa ja vaivannäköä. Jos lomake on suunniteltu huolellisesti, aineisto voidaan nopeasti käsitellä haluttuun muotoon ja analysoida tietokoneen avulla. Myös aikataulu ja kustannukset voidaan arvioida melko tarkasti. (Hirsjärvi, Remes & Sajavaara 2000: 182)

Kyselylomaketutkimuksen huonona puolena pidetään usein sitä, että vastausprosentti jää huonoksi. Tämän takia me yhdistimme työssämme sekä kyselylomaketutkimuksen ja haastattelun. Kyselyyn osallistujille annoimme lomakkeen henkilökohtaisesti ja olimme käytettävissä mahdollisia lisäkysymyksiä varten.

Haastattelun suurena etuna muihin tiedonkeruumuotoihin verrattuna on se, että siinä voidaan säädellä aineiston keruuta joustavasti tilanteen edellyttämällä tavalla ja vastaajia myötäillen. Haastatteluaiheiden järjestystä on mahdollista säädellä, samoin on enemmän mahdollisuuksia tulkita vastauksia kuin esimerkiksi postikyselyssä. (Hirsijärvi yms. 2000: 192)

4.2 Työvaiheiden kuvaus

Alussa olimme yhteydessä toimeksiantajaamme ja saimme heiltä aiheen tutustua tietoturvaan ja tehdä myymälöille ja varastolle yleiset tieturvaohjeet. Toimeksiantajalla ei ollut myymälä- ja varastohenkilökunnalle mitään tieturvaohjeita ja resurssit niiden tekemiseen olivat vähäiset. Saimme opinnäytetyön aiheen toimeksiantajalta ja työn rajaus tuli myös toimeksiantajan tarpeen mukaan. Ohjeitten ja tietoturvan nykytilan kartoituksen kannalta atk-osasto olisi ollut mielenkiintoisempi, koska suurin osa Vapaa Valinnan teknisestä puolesta tai tietoturvapäätöksistä hoidetaan atk-osaston kautta.

Aloitimme kirjallisuuden etsimisen ja siihen tutustumisen. Materiaalia etsimme kirjoista, lehdistä ja Internetistä. Samalla mietimme, miten hyödynnämme hen-

kilökuntaa ja mitä tietoja yritämme saada kyselymme perusteella henkilökunnalta. Atk-osastolta saimme tiedon, että tilanne kaikissa myymälöissä on samantapainen, eli kaikissa myymälöissä ei tarvinnut käydä haastattelemassa.

Keräsimme tietoa yrityksen tietoturvan nykytilasta kyselylomakkeiden ja haastatteluiden avulla. Sopivien kysymysten miettiminen kyselylomakkeeseen oli hankalaa. Oli vaikeaa miettiä, millaisilla kysymyksillä saamme parhaiten kattavaa tietoa. Päätimme tehdä kyselylomakkeen tietoturvan eri osa-alueet mahdollisimman monipuolisesti huomioon ottaen. Se on jaettu kahdeksaan osa-alueeseen Suomen valtiohallinnon tietoturva määritelmän mukaisesti. Nämä osa-alueet ovat: fyysinen turvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus, käyttöturvallisuus, henkilöstöturvallisuus, hallinnollinen tietoturva ja tietoliikenneturvallisuus. Näiden osa-alueiden alle rakensimme kysymykset. Kysymyksillä halusimme saada vastauksia myymälöiden ja varaston tämänhetkisistä toimintatavoista, jotta mahdolliset puutteet ja muutostarve selviäisi. Kyselylomakkeiden avulla halusimme myös kartoittaa, millaisille ohjeistuksille myymälöissä ja varastossa on tarvetta.

Käytimme kvalitatiivista tutkimusmenetelmää, koska lähtötilanne eri myymälöissä on melko sama. Tutkimuksessa hyödyimme enemmän siitä, että olimme paikanpäällä haastattelemassa ja vastaamassa mahdollisiin lisäkysymyksiin, kuin esimerkiksi koko henkilökunnan täyttämään Internet-lomakkeeseen. Haastatteluissa työntekijöillä oli mahdollisuus myös kertoa toiveista tulevaa ohjeistusta ja toimenpiteitä varten. Haastattelutekniikkana oli yksilöhaastattelu. Yksilöhaastattelu eteni lähinnä kyselylomakkeen pohjalta esille tulleiden asioiden pohjalta sekä haastateltavien toiveiden pohjalta. Haastattelut olivat hyvin vapaamuotoisia, eli vapaalle keskustelulle ja lisäkysymyksille oli mahdollisuus. Kyselylomakkeiden ja haastatteluiden avulla saimme kerättyä tietoa yrityksen tietoturvan nykytilasta.

Haastattelemamme henkilöt täyttivät ensin kyselylomakkeen, jonka jälkeen haastattelimme näitä henkilöitä vielä joidenkin kysymysten osalta suullisesti ja teimme niistä erilliset muistiinpanot. Näin saimme hyvin lisätietoa asioista, joita emme olleet huomanneet kyselylomakkeessa kysyä, ja heillä oli myös mahdollisuus sanoa omia mielipiteitään ja kehitysehdotuksia. Haastattelut teimme neljään myymälään, Koskikeskuksen, Tammelan, Valkeakosken ja Millerin myymälään Kylmäkoskella. Haastattelimme myös Vapaa Valinnan varastolla kahta henkilöä ja konttorista Vapaa Valinnan atk-päällikköä eli yhteensä seitsemää henkilöä. Toimeksiantajan mukaan kaikilla myymälöillä on samanlainen lähtötilanne tietoturvaohjeiden ja toimintatapojen suhteen, tämän vuoksi he eivät nähneet tarpeelliseksi haastatella kaikkia myymälöitä.

Kyselylomakkeiden purkaminen oli yksi mittava työvaihe. Analysoimme kysymys kerrallaan kyselytutkimuksen tuloksen ja huomasimme, että vastaukset olivat melko samanlaisia kaikilla haastatteluun osallistuneilla lukuun ottamatta atk-päällikköä. Kirjasimme ylös tässä vaiheessa osa-alue kerrallaan esiin tulleita asioita. Kirjoitimme osa-alueitten osalta tulokseksi ne kohdat, joihin myymälä- ja varastohenkilökunnalla oli mielipide. Moneen kysymykseen tuli vas-

taukseksi ”en tiedä” -vaihtoehto, koska atk-osasto hoitaa suurimman osan Vapaa Valinnan tietoteknisistä asioista. Haastatteluissa kysyimme henkilökunnalta toiveita koulutukseen ja vastasimme heille kyselylomakkeesta heränneisiin kysymyksiin. Näin saimme purettua yrityksen tämän hetkisen tietoturvan tilan. Yleistimme tutkimustuloksen koskemaan kaikkia myymälöitä samankaltaisten vastausten perusteella. Haastattelemamme henkilöt kertoivat myös, että kaikissa myymälöissä tilanne on samankaltainen.

Tulosten analysoinnin jälkeen aloimme miettiä tietoturvaohjeistusta myymälöille sekä varastolle ja kirjoittamaan opinnäytetyötämme. Myymälä- ja varastohenkilökunnan ohjeet toivottiin tässä vaiheessa niin yleisiksi, että ne sopivat kaikille ja toimeksiantaja tarkentaa niitä tarpeen mukaan. Konttorille tai atk-osastolla on jo omat tarkemmat ohjeet olemassa.

Teimme opinnäytetyömme yhdessä ja jaoimme työt puoliksi. Tämä onnistui mielestämme hyvin. Kaikki haastattelut ja tulosten analysoinnit teimme yhdessä ja kirjoitusosuutta jaoimme aina kappale kerrallaan ja tarkistimme tulosta yhdessä.

5 Johdatus Vapaa Valinnan tietoturvaohjeistoon

Tässä kappaleessa selvennetään, mitä kyselylomakkeilla on haluttu tietää Vapaa Valinnan tietoturvasta eri osa-alueilla. Kyselylomake on tehty tietoturvan eri osa-alueet mahdollisimman monipuolisesti huomioon ottaen ja se on jaettu kahdeksaan osa-alueeseen, näiden osa-alueiden alle on tehty kysymykset. Kysymyksillä on haluttu saada vastauksia myymälöiden ja varaston tämänhetkisistä toimintatavoista, jotta mahdolliset puutteet ja muutostarve selviäisi. Kyselylomakkeiden avulla on haluttu myös kartoittaa, millaisille ohjeistuksille myymälöissä ja varastossa on tarvetta.

Vapaa Valinnassa hallinnollinen tietoturva on lähinnä johtoryhmän ja atk-osaston hoidettavissa, mutta tässä on kartoitettu, onko myymä- ja varastohenkilökunnalla siitä osa-alueesta mitään tietoa. Vaikka asiat päätetään lähinnä johtoryhmässä ja atk-osastolla, muulla henkilökunnalla olisi hyvä olla perustietämys asioista. Hallinnollisen tietoturvan kysymyksillä on haluttu kartoittaa, mistä ja millaista ohjeistusta henkilökunta kaipaisi.

Fyysinen turvallisuus koskee kaikkia työntekijöitä yrityksessä ja on siksi tärkeä osa-alue kaikille työntekijöille. Fyysisen turvallisuuden kysymyksillä on haluttu kartoittaa toimitilojen turvallisuutta ja kulunvalvontaa. Kysymyksillä on myös kartoitettu esimerkiksi, onko myymälöissä ja varastolla hälytysjärjestelmää, sammutusjärjestelmää ja paloilmoitinjärjestelmää. Nämä kaikki ovat tärkeitä turvallisuuteen liittyviä asioita, jotka vaikuttavat myymälöiden ja varaston fyysiseen turvallisuuteen.

Laitteistoturvallisuudessa on mietitty, onko myymälähenkilökunnalla tiedossa esimerkiksi käyttäjätunnuksien ja salasanojen merkitys koneiden suojaamiseksi. Käyttäjätunnus ja salasana ovat merkittäviä laitteistoturvallisuuteen liittyviä tekijöitä Vapaa Valinnassa, koska useimmissa myymälöissä laitteet on sijoitettu myymälätiloihin. Myös salasanojen vaihto riittävän usein on tärkeää. Kysymyksillä on myös selvitetty, miten toimitaan laitevian tai muun vastaavan sattuessa.

Ohjelmistoturvallisuus-osiossa on kartoitettu, onko henkilökunnalla tietoa haittaohjelmista ja viruksista sekä niiden torjunnasta Vapaa Valinnassa. Tarkoituksena oli myös selvittää, osaavatko työntekijät toimia oikein viruksen tai haittaohjelman yllättäessä. Tärkeää oli myös kartoittaa, onko kaikilla työntekijöillä käyttöoikeudet eri ohjelmistoihin.

Tietoaineistoturvallisuus kysymyksillä on selvitetty, millaiset tiedot henkilökunnalla on tietojen käsittelystä, kuten säilytyksestä, siirrosta, kopioinnista, hävittämisestä ja jakelusta. Henkilökunnalta kysyttiin myös yrityksen tietokannoista ja niiden käyttöoikeuksista. Tietoaineistoturvallisuuden kannalta on tärkeää myös, että henkilökunta tietäisi, mitkä aineistot ovat luottamuksellisia, jotta niitä osattaisiin käsitellä oikein.

Käyttöturvallisuus-osion tarkoituksena on kartoittaa työntekijöiden järjestelmien käyttöperiaatteita. Varmuuskopiointi on tärkeää yrityksen käyttöturvallisuuden kannalta, jotta tärkeät tiedot säilyvät varmasti. Jokaisella työntekijällä on hyvä olla varamies, joka osaa toisen työtehtävät. Yrityksen on hyvä luoda sellaiset menettelytavat, joilla päivittäisessä toiminnassa säilytetään tietoturvallisuuden taso mahdollisimman hyvänä.

Henkilöstöturvallisuus-alueen kysymyksillä on haluttu saada selville henkilökunnan liikkumiseen ja tunnistamiseen liittyvät seikat. On selvitetty myös, miten toimitaan uusien ja lähtevien työntekijöiden kanssa. Työntekijöiden vastuujaot on tärkeää määritellä tasaisesti. Tärkeänä on myös pidetty henkilökunnan kouluttamiseen kohdistuvia kysymyksiä. Motivaatiosta ja kouluttamisesta on kysytty lisää haastatteluiden avulla.

Tietoliikenneturvallisuus-alueen kysymyksien tarkoituksena on selvittää, miten koneet ja tietoliikenneyhteydet on myymälöissä suojattu, ja kuinka paljon henkilökunnalla on tietoa niiden suojauksesta. Haastatteluiden avulla on myös kartoitettu, olisiko myymälöissä ja varastolla hyödyllistä olla Internet-yhteys.

Osa-alueissa kysymykset ja aiheet menivät osittain päällekkäin. Ohjelmisto-, tietoaineisto-, käyttö- ja tietoliikenneturvallisuuden kysymyksiin osasi tyhjentävästi vastata vain atk-päällikkö, koska atk-osasto hoitaa kaikki näihin liittyvät toimet Vapaa Valinnassa. Kysymyksillä on haluttu kuitenkin tietoa siitä, minkälaista perustietoa henkilökunnalla on tietoturvasta ja mistä henkilökunta haluaa tietää lisää.

Vapaa Valinnan tietoturvaohjeistuksessa on käytetty apuna kappaleessa kolme mainittuja kysymyksiä soveltuvin osin. Tämän tyylisiin ohjeistuksiin tai oppaaseen ei löytynyt paljon lähdemateriaalia. Joihinkin tietoturvan osa-alueisiin on lisätty huomioitavia asioita, kuten henkilöstöturvallisuuteen. Hyvät tietoturvaohjeet on tehty kohderyhmälle sopiviksi ja ymmärrettäviksi.

6 Tutkimustulos

6.1 Kyselylomakkeiden ja haastatteluiden purkaminen

Analysoimme haastatteluiden tulokset osa-alue kerrallaan. Kyselylomakkeiden ja haastatteluiden purkaminen oli vaikeampaa kuin olimme ajatelleet. Purimme niitä kysymys kerrallaan ja teimme jokaisesta kysymyksestä yhteenvedon, jossa analysoimme tuloksen. Huomasimme, että vastaukset olivat hyvin samankaltaisia joitain poikkeuksia lukuun ottamatta. Poikkeuksia olivat lähinnä atk-päälliköltä saamat vastaukset. Keräsimme vastaustulokset osa-alue kerrallaan yhteen ja kirjoitimme tuloksen jokaisesta osa-alueesta. Vastauksissa oli paljon vaihtoehtoa ”en tiedä”. Tämä kertoi siitä, että myymälä- ja varastohenkilökunnalla on aika vähän tietoa yrityksen tietoturvasta. Monet mielsivät, että tietoturva koskee vain koneisiin liittyviä asioita. Vastauksista ilmeni, ettei heillä ole paljon tietoutta siitä, mitä tietoturvallisuus pitää sisällään. Haastatteluissa lähes kaikki sanoivat kaipaavansa selkeitä ohjeita ja koulutusta tietoturvasta ja muista asioista, kuten esimerkiksi atk-laitteistoista. Tässä vaiheessa myymälöiden ja varaston tietoturvan nykytila alkoi selkiytyä. Näiden tietojen perusteella pystyimme aloittamaan tietoturvaohjeistuksen hahmottelua. Myymälöihin ja varastolle tehty kyselylomake on liitteenä 2.

6.1.1 Hallinnollinen tietoturva

Hallinnollinen tietoturva muodostaa perustan tietoturvatoiminnalle. Se on tietoturvallisuuden toteuttamista että johdon ja henkilöstön sitoutumista tietoturvallisuuden järjestelmälliseen kehittämiseen ja hoitamiseen. Hallinnollinen tietoturva koostuu johdon hyväksymistä periaatteista, vastuun jaosta, tarkoitukseen varatuista resursseista sekä riskien arvioinnista.

Kyselytutkimuksen perusteella voidaan todeta, että Vapaa Valinnan myymälä- ja varastohenkilökunnalta puuttuu yksityiskohtainen ohjeisto hallinnollisen tietoturvan osa-alueista. Yrityksen tietoturvapolitiikkaa ei ole määritelty, joka pitäisi sisällään näkemyksen tietoturvan päämääristä, periaatteista ja toteuttamisesta. Vapaa Valinnassa tietoturvavastuut on jaettu lähinnä atk-osastolle. Tämän vuoksi muun henkilökunnan ei ole tarvinnut käsitellä näitä asioita. Mielestämme myymälöissä ja varastolla pitäisi olla henkilö tai henkilöitä, jotka ovat perehtyneet tietoturva-asioihin.

Myymälä- ja varastohenkilökunnalle on jaettu vuosien varrella yksittäisiä ohjeita liittyen tietoturvapolitiikkaan ja -ohjeistukseen. Näitä ohjeita ei ole monessakaan myymälässä säilytetty asianmukaisesti. Uudelle työntekijälle kerrotaan perehdyttämisvaiheessa, mitkä tiedot ovat salaisia ja mitkä yleisiä. Yleisesti ottaen yrityksen salaiset, esimerkiksi päivän myyntiä koskevat tiedot, ovat henkilökunnan tiedossa. Tämän voisi muuttaa esimerkiksi niin, että nämä tie-

dot olisivat myymäläpäällikön ja varavastaavan tiedossa. Muulle henkilökunnalle voisi antaa tiedon hyvästä tuloksesta ilman tarkkoja summia.

Yrityksessä on suojattu kassakoneet ja myymälässä oleva tietokone käyttäjätunnuksin ja salasanoin. Kassakoneisiin kaikilla on omat salasanat ja käyttäjätunnukset, mutta myymälässä olevalle koneelle kaikki kirjautuvat samalla käyttäjätunnuksella ja salasanalla. Henkilökunta tiesi myös hyvin, että koneet on suojattu varavoimajärjestelmällä. Muista suojattavista kohteista kuten verkko, tietokanta tai järjestelmä ei myymälä- ja varastohenkilökunnalla ollut tietoa.

Tietoturvaan liittyvät vastuukysymykset koskevat vain harvoin myymälä- ja varastohenkilökuntaa. Haastatteluissa tuli ilmi, että vahingon sattuessa vastuut mietitään jälkikäteen tapauskohtaisesti.

6.1.2 Fyysinen turvallisuus

Fyysisen turvallisuuden tärkein tehtävä on suojata järjestelmiä erilaisilta fyysisiltä uhkilta ja vahingoilta, jotka voivat olla ihmisten aiheuttamia tai luonnonilmiöistä johtuvia. Fyysinen turvallisuus on sekä rakenteellista turvallisuutta, kuten lukitus, palo- ja vesivahinkojen suojaaminen, että rikostorjuntaan liittyvää turvallisuutta, kuten kameravalvonta. Fyysinen turvallisuus tulee huomioida jo rakennuksen suunnitteluvaiheessa.

Yrityksessä on huomioitu seuraavat kulunvalvontaan liittyvät seikat: varashälyttimet, murtohälyttimet, kameravalvonta, henkilökunnan poistumistarkastukset, vain työntekijöillä on avaimet yrityksen tiloihin, tavarantuojalla oma murtohälytinkoodi oveen, siivoojat käyvät yrityksen aukioloaikoina ja vartija kierrokset. On tärkeää, että laitteet, esimerkiksi varashälyttimet, murtohälyttimet ja kameravalvonta toimivat. Näin ollen näitä pitäisi aika ajoin testata. Muuten kulunvalvonta Vapaa Valinnassa on mielestämme hoidettu hyvin.

Tutkimuksesta selvisi, että yrityksen ulko-ovet ovat lukittuna aina myymälöiden ja varaston ollessa kiinni ja henkilökunnan tiloihin menevät ovet ovat aina myymälöissä lukittuina. Myymälöissä ja varastossa on palovaroittimet ja sammutusjärjestelmät, mutta kaikki työntekijät eivät tienneet sammutusjärjestelmästä. Yrityksellä ei ole käytössään vieraiden seurantalistaa, mutta vieraat saavat kulkea henkilökunnan tiloissa vain jonkun työntekijän seurassa ja vierailta pitäisi tarkistaa henkilökortti.

Suurimmassa osassa myymälöitä tietokoneet on sijoitettu myymälätiloihin, vain harvassa myymälässä ne olivat lukitussa tilassa. Myymälässä olevalle tietokoneelle on siis mahdollisuus päästä ulkopuolisen henkilön. Tietokoneet ja kassapäätteet tuleekin aina olla lukittuna niiltä poistuttaessa edes hetkeksi.

6.1.3 Laitteistoturvallisuus

Laitteistoturvallisuus tarkoittaa, että laitteet on inventoitu, niiden sijainnista ja kokoonpanosta ollaan selvillä ja niiden varaosien saanti sekä kriittiset järjestelmät on turvattu. Tämä voi käsittää esimerkiksi laitteiden kahdentamisen ja energian saannin varmistamisen sekä huoltosopimuksista huolehtimisen.

Yrityksessä laitteistoihin pääsy on toteutettu käyttäjätunnuksella ja salasanalla. Myymälätiloissa oleville koneille kaikilla työntekijöillä on yhteiset tunnukset ja kassakoneille kaikilla työntekijöillä on omat tunnukset. Laitteistojen tunnuksia ei ole vaihdettu tarpeeksi usein, ovikoodit vaihdetaan säännöllisesti.

Myymälöiden ja varaston tietokoneilla pystyy muuttamaan toisten tietoja muutkin kuin järjestelmänhoitaja. Tietokoneelle voi päästä jopa ulkopuolinen henkilö muuttamaan tietoja, jos se on lukitsematta. Myymälätiloissa oleva tietokone ei ole aina näppäinlukittu, tietoturvallisuuden kannalta tietokoneet tulisi aina lukita siltä poistuttaessa. Kassakoneet ovat pääsääntöisesti aina lukittu niiltä poistuttaessa, tämä pitäisi toteutua vaikka kassalta poistuisi vain hetkeksi.

Laitteistovian sattuessa kyseinen laite pystytään korvaamaan kohtuullisen nopeasti tilanteesta riippuen, yleensä vuorokauden sisällä. Laitteistovian sattuessa tulisi heti ilmoittaa siitä vastaavalle henkilölle. Kaikilla laitteilla on varavirtajärjestelmät esimerkiksi sähkökatkoksien varalle. Tutkimuksesta ilmeni, että myymälä- ja varastohenkilökunta tiesi hyvin varavirtajärjestelmästä.

6.1.4 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudessa on kyse käyttöjärjestelmien ja sovellusohjelmien turvallisuusominaisuuksista sekä niiden käyttömahdollisuuksista. Siihen kuuluvat ohjelmistojen pääsynvalvonta, virustorjunta sekä tietojärjestelmien tapahtumatietojen kirjaaminen.

Yrityksellä on palomuuri ja viruksentorjuntaohjelma, mutta työntekijöillä ei ole tietoa ohjelmista. Viruksentorjuntaohjeita ei ole, joten henkilökunta ei välttämättä osaa toimia haittaohjelman tai viruksen yllättäessä. Atk-osasto hoitaa virustarkistukset, jotka tehdään ainakin kerran vuorokaudessa. Haastatteluissa tuli ilmi, että henkilökunta haluaisi koulutusta ja lisää tietoa viruksista, haittaohjelmista ja viruksentorjunnasta. Tärkeimpien ohjelmistojen tapahtumatiedot kirjataan suojattuun lokitiedostoon, mutta tiedostojen salaamista tiedostoissa ei käytetä. Atk-osasto huolehtii ohjelmistojen päivittämisestä, joten tämä asia ei koske myymälä- ja varastohenkilökuntaa. Yrityksen ohjelmistojen cd:t ovat oikein säilytettynä, mutta ohjelmistojen käsikirjoja ja lähdekoodeja ei kaikista ole ja lisenssiluetteloa ei ole tehty.

Vapaa Valinnassa on käytössään Merx-toiminnanohjausjärjestelmä. Merx on suuressa osassa henkilökunnan jokapäiväisissä työtehtävissä. Sillä henkilökunta voi tehdä ostotilauksia, saavuttaa tuotteet myymälän saldoille, inventoida ja

nähdä varastosaldot ja tehdä ostajan tuotekyselyn, jolla saadaan paljon lisää tietoa tuotteesta. Raportointi-ohjelmalla saadaan myymälän päiväkohtaiset myyntitiedot, kassapäätteillä tehdyt palautukset ja korjaukset.

Tällä hetkellä myymälöiden sähköpostijärjestelmä on vain yrityksen sisäinen. Henkilökunta toivoisi, että sähköpostia voisi lähettää yrityksen ulkopuolelle ja vastaanottaa yrityksen ulkopuolelta tullutta postia. Henkilökunta toivoi myös Internet-yhteyttä myymälöihin ja varastolle. Mielestämme se on nykyaikainen media, jota on turhaan vältetty epäillen väärinkäyttöä. Internetin hyödyt ovat kuitenkin suuremmat kuin satunnainen väärinkäyttö. Internetin käytöstä voisi laatia tarkat ohjeet, jos se asennettaisiin myymälöihin.

Yrityksen Internet-sivut on suojattu, niin etteivät ulkopuoliset pysty niitä muuttamaan, henkilökunta ei tosin sitä tiennyt.

6.1.5 Tietoaineistoturvallisuus

Tietoaineistoturvallisuuteen liittyvät tiedon jatkuva varmistaminen, asianmukainen säilytys sekä hävittäminen. Tietoaineistoturvallisuudella pyritään säilyttämään asiakirjojen, tietueiden ja tiedostojen luottamuksellisuus sekä estämään tietojen tuhoutuminen tai tahaton muuttuminen. Oleellista on tallenteiden suojaaminen ja oikeanlainen säilyttäminen.

Yrityksellä ei ole yhtenäisiä ohjeita koskien tietojen säilytystä, siirtoa, kopiointia, hävittämistä ja jakelua. Näistä on tullut vain erillisiä tiedotteita, joita kaikki myymälät eivät ole säilyttäneet. Yksittäisiä tiedotteita on melkein mahdotonta säilyttää niin, että ne olisivat nopeasti käytettävissä. Jokaisella myymälällä on oma toimintatapa, jonka mukaan on toimittu vuosia. Mielestämme tähän voisi olla kehitysideana Tokmanni-konsernin yhteinen intranet-sivusto organisaation tiedonvälitykseen. Jokaiselle eri liikkeelle, kuten esimerkiksi Vapaa Valinnoille ja Tokmanneille, olisi omat sivut. Sillä saisi vaivattomasti tiedottaa asioista ja se olisi hyvä myös tiedon/tiedotteiden arkistointiin. Myymälöiden ja varaston ei tarvitsisi pitää enää kaikista ohjeistuksista tai tiedotteista paperiversioita.

Myymälöillä ja varastolla on käytössään kattavat tuotetietokannat, Merx-toiminnanohjausjärjestelmä sekä kassojen omat tietokannat. Näihin myymälöissä ja varastolla on koko henkilökunnalla samat oikeudet. Yrityksen tietoja tallennetaan mikrofilmille, paperille ja cd:lle. Myymälässä tiedot tallennetaan lähinnä paperille.

Luottamuksellisia ja salaisia tietoja sisältävä tietokantapalvelin on suojattu palomuurilla ja pääsyoikeuksilla. Tietokantapalvelin on yhteydessä Internetiin. Asiakkaan luottamukselliset tiedot ovat turvassa ja tietoliikenteen kautta kulkeva tieto on salattu.

6.1.6 Käyttöturvallisuus

Käyttöturvallisuus koostuu monesta asiasta; järjestelmien turvallisista käyttöperiaatteista, tietojenkäsittelytapahtumien valvonnasta sekä jatkuvuuden turvaamisesta. Periaatteena on luoda sellaiset menettelytavat, joilla päivittäisessä toiminnassa säilytetään tietoturvallisuuden taso mahdollisimman hyvänä. Mielestämme tämä osa-alue pitää sisällään paljon jo muissa osa-alueissa tarkemmin esiteltyjä kohtia.

Yrityksen työntekijöillä on myymäläkohtaiset tunnukset tietokoneille ja heillä on niihin kaikki oikeudet. Mielestämme henkilökunnan oikeuksia koneille ja eri ohjelmistoihin tulisi määritellä työntekijän tehtävän mukaan. Merx-toiminnanohjausjärjestelmään pitäisi jokaiselle työntekijälle perustaa omat käyttäjätunnukset ja salasanat, jotta käyttäjä pystyttäisiin tunnistamaan. Henkilökunnalla ei ole tietoa, miten varmuuskopiointi on hoidettu. Atk-osasto hoitaa varmuuskopioinnin ja se suoritetaan kerran päivässä.

Työntekijöiden pitäisi periaatteessa osata toistensa työt, jotta kaikilla olisi varamies yllättävien poissaolojen varalle. Haastattelussa ilmeni, että näin ei kuitenkaan aina ole kaikkien työtehtävien suhteen.

6.1.7 Henkilöstöturvallisuus

Henkilöstöturvallisuuden avulla organisaatio pyrkii torjumaan henkilöstöstä aiheutuvia tai henkilöstöön kohdistuvia uhkatekijöitä. Toimenpiteet ulottuvat vakinaiseen ja tilapäiseen henkilöstöön Henkilöstöturvallisuus käsittää koko henkilöstön liikkumiseen, matkustamiseen ja tunnistamiseen liittyvät seikat, mutta myös yksityisyyden suojaan, taustojen tarkistamiseen, motivaation ylläpitämiseen ja kouluttamiseen. Koskivirta (2006) painottaa henkilöstön motivoinnin tärkeyttä artikkelissaan. Hän sanoo, että yritys onnistuu tietoturvansa hoitamisessa vain, kun henkilöstöllä on motivaatio käyttäytyä tietoturvallisesti.

Ennen työntekijän palkkaamista henkilön taustatiedot tarkistetaan. Työsuhteen päättyessä kyseisen henkilön kulkuluvat sekä käyttöoikeudet poistetaan. Tämä saattaa joskus kestää hieman kauemmin kuin pitäisi. Olisi hyvä, että oikeudet järjestelmiin ja ohjelmistoihin poistettaisiin työntekijän viimeisenä työpäivänä.

Työntekijöiden kesken ei ole jaettu tietoturvavastuita, koska atk- ja turvallisuusosasto hoitaa ne. Kuitenkin myymälöissä ja varastolla olisi hyvä olla useampi kuin yksi henkilö, jotka olisivat perehdytetty tarkemmin tietoturvaasioihin. Henkilökunnan kesken pitäisi työt olla jaettu tasapuolisesti, mutta joskus tämä ei kuitenkaan toteudu. Henkilökuntaa koulutetaan poikkeustilanteita varten. Haastatteluissa tuli esille esimerkiksi turvallisuuskoulutus, palontorjunta, ensiapukoulutus ja yrityksen oman toiminnanohjausjärjestelmän käyttökoulutusta.

6.1.8 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus tarkoittaa siirrettävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaamista tietojen siirron aikana. Tähän osa-alueeseen kuuluu mm. salaus, verkon palveluvarmuuden turvaaminen, turvallisen reitityksen järjestäminen, vain sallittujen palveluiden salliminen, vaihtoehtoisten tiedonsiirtotapojen suunnittelu, yksityisyyden suoja yms.

Yritys on varautunut käyttämään vaihtoehtoisia tiedonsiirtotapoja, kuten faksia, postia ja yrityksen sisäistä postia, konerikkojen tai muun vastaavan sattuessa. Yrityksellä on käytössä palomuuriohjelma ja sen tietoliikenneyhteydet on suojattu salauksin sekä suljetulla yritysverkolla. Koneilta on karsittu kaikki turhat palvelut, jopa www-palvelin. Tietoliikenteellä on varmistukset tai vaihtoehtoiset reitit katkon sattuessa.

Myymälähenkilökunta ei osannut vastata tietoliikenneturvallisuutta koskeviin kysymyksiin juuri lainkaan. Atk-osasto onkin suurimmassa osassa vastuussa tämän alueen toiminnasta. Tämänkin osa-alueen asioista voisi henkilökunnalle kertoa yleiset toimintaperiaatteet.

7 Yleistä Vapaa Valinnan tietoturvaohjeistuksesta

Tekemämme tietoturvaohjeistus on tarkoitettu jokaisen työntekijän käyttöön, siksi ohjeistus on laadittu tarpeeksi yleiseksi. Tietoturvaohjeistus on liitteenä 1. Ohjeistus on tarkoitettu nimenomaan myymälä- ja varastohenkilökunnalle, joilla ei ole aiempaa tietoa tietoturvasta ja siihen liittyvistä aihealueista. Tietoturva-asioista vastaa atk-osasto, joten myymälähenkilökunnan ei ole tarvinnut olla näiden asioiden kanssa tekemisissä. Koko henkilökunnalla on kuitenkin hyvä olla perustietämys tietoturva-asioista ja selkeät ohjeet joidenka avulla toimia. Tälläkään osa-alueella henkilökunnan koulutus ei ikinä mene hukkaan.

Myymälöillä ja varastolla ei ole määritelty tietoturvapolitiikkaa. Tietoturvapolitiikka on yrityksen johdon hyväksymä näkemys tietoturvan päämääristä, periaatteista ja toteuttamisesta. Vapaa Valinnan johdon tai atk-osaston tulisi määritellä yrityksen tietoturvapolitiikka. Johdon tai atk-osaston tulisi myös antaa tarkat ja yhtenäiset ohjeet käytännön toimenpiteisiin. Ohjeita tulee päivittää tarpeen mukaan ja toimittaa aina päivitetyt ohjeet myymälöille. Näin myymälöihin ei kasaannu yksittäisiä ohjelappusia, joiden säilytys on myymäläkohtaista. Ohjeet tulee käydä läpi henkilökunnan kanssa tarkasti ja kerrata niitä päivitysten jälkeen. Ohjeiden tulee olla jokaisen työntekijän saatavilla tarvittaessa.

Myymälöiden ja varaston fyysiseen turvallisuuteen liittyvät asiat tulee olla aina kunnossa. Eli toimitiloissa on pidettävä huolta, että murto- ja varashälyttimet sekä paloilmoitinjärjestelmä ovat toiminnassa. Hätätilanteita varten normaalit ja poikkeusreitit tulee olla selkeästi määriteltyinä. Henkilökunnan tulee myös kiinnittää huomiota vierailijoiden ja edustajien kulkemiseen toimitiloissa.

Laitteistoturvallisuudella suojataan yrityksen laitteistojen väärinkäyttö. Tietokone ja kassakone on lukittava aina niiltä poistuttaessa. Myymälän tietokoneen kanssa tulisi noudattaa erityistä huolellisuutta, jos se on sijoitettu myymälätiloihin, eikä lukittuun tilaan. Laitteistot on suojattu käyttäjätunnuksin ja salasanoin. Laitteistojen salasanat tulee vaihtaa säännöllisin väliajoin. Vielä nyt salasanoja ei kuitenkaan vaihdeta säännöllisin väliajoin, vaikka sen voisi toteuttaa yksinkertaisella menetelmällä. Salasanojen vaihdon voisi toteuttaa esim. salasanojen vanhentumisella, jolloin jokainen, jolla on oma salasana voi vaihtaa sen järjestelmän ilmoittaessa uuteen. Hyvä salasana on sellainen, joka ei ole johdettavissa, ei liity henkilökohtaiseen elämään, on riittävän pitkä ja sisältää isoja ja pieniä kirjaimia. On myös hyvä käyttää eri salasanaa eri paikoissa.

Ohjelmistoihin olisi tärkeää määritellä kaikille työntekijöille omat käyttäjätunnukset ja salasanat. Merx:iin ja raportointi-ohjelmaan tulisi määritellä rajattu käyttöoikeus henkilökunnan tehtävien mukaan, esimerkiksi kausiapulaisilla ei tarvitse olla kaikkia oikeuksia. Kun jokaisella työntekijällä on omat tunnukset ohjelmistoihin, pystyttäisiin tarvittaessa tunnistamaan käyttäjä. Ohjelmistoihinkin salasanat tulisi vaihtaa säännöllisin väliajoin. Henkilökunta toivoi tietoa haittaohjelmista ja viruksista sekä niiden torjunnasta.

Myymälöille ja varastolle tulisi olla yhtenäinen ohje tietojen käsittelyyn. Ohjeet tulisi päivittää säännöllisesti, varsinkin jos toimintatapoihin tulee muutoksia. Kaikki luottamukselliset aineistot tulee säilyttää lukkojen takana, jottei aineisto joudu ulkopuolisille. Yrityksen kassapäätteillä ja tietokoneilla on paljon luottamuksellista tietoa, joten on tärkeää aina lukita kone siltä poistuttaessa edes hetkeksi.

Kaikki tehtävät pitää jakaa niin, että tehtävillä on vähintään kaksi osaajaa. Jos vastuuhenkilö esimerkiksi sairastuu, osaa joku tehdä hänen työnsä. Joka myymälöissä ja varastolla tulisi muutama henkilö perehdyttää tarkemmin tärkeisiin osa-alueisiin, kuten Merx:in käyttöön ja tietoturva-asioihin. Myymälöissä tulisi olla myös henkilö, joka on perehdytetty tarkemmin kassajärjestelmään. Näin olisi mahdollisuus saada ohjeistusta tai neuvoa helpommin ja nopeammin.

Kyselytutkimuksen mukaan esimerkiksi viruksista halusi tietoa useampi myymälä. Viruksista henkilökunta halusi yleistä tietoa sekä keinoja, miten välttää niitä, ja mitä pitäisi tehdä, jos koneelle pääsee virus.

Kyselytutkimuksesta selvisi, että lähes kaikista tietoturvanosa-alueista henkilökunta haluaisi tai tarvitsisi koulutusta. Koulutuksessa voisi kertoa yrityksen yleiset tietoturvakäytännöt, kerrata yleisiä sääntöjä ja käydä läpi atk-laitteistot ja niiden käyttö.

Henkilökunnan vastuut tulisi jakaa tasaisesti myymälöissä ja varastolla. Uuden työntekijän taustatiedot tulisi tarkistaa ja jokainen uusi työntekijä allekirjoittaa työsopimuksen. Käyttäjätunnukset ja salasanat pitäisi perustaa ennen uuden työntekijän ensimmäistä työpäivää, jotta hän pystyy aloittamaan työt heti. Uuden työntekijän työhön perehdyttämisen yhteydessä kerrotaan Vapaa Valinnan tietoturvaan liittyvät säännöt ja määräykset. Työsuhteen päättyessä Vapaa Valinnassa poistetaan työntekijän käyttöoikeudet järjestelmistä, poistetaan kulkuoikeudet, palauttaa Vapaa Valinnan avaimet ja hänen työnsä tulee jakaa asianmukaisesti muille työntekijöille sekä tiedottaa asiasta muita työntekijöitä.

8 Yhteenveto

Tietoturva on osa-alueena hyvin laaja käsite ja siihen liittyvät riskit ovat vaikeita hallita. Olemme jakaneet tietoturvan työssämme Suomen valtiohallinnon virallisen määritelmän (nk. sipulimalli) mukaan kahdeksaan osa-alueeseen. Neljä ulointa kerrosta ovat: hallinnollinen tietoturva, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus. Näiden neljän kerroksen suojaamana ovat sisimpänä: ohjelmistoturvallisuus, tietoaineistoturvallisuus, käyttöturvallisuus, laitteistoturvallisuus. Nämä osa-alueet auttavat ymmärtämään paremmin mitä tietoturva tarkoittaa.

Asetimme työmme tavoitteeksi saada selville myymälöiden sekä varaston tietoturvan nykytilan ja sen pohjalta tehdä yleinen tietoturvaohjeistus myymälöiden ja varaston henkilökunnalle. Mielestämme nykytilan kartoitus onnistui hyvin kyselylomakkeiden ja haastatteluiden avulla. Kyselomaketta tehdessämme mietimme turhan monimutkaisesti kysymyksiä. Haastatteluissa huomasimme, että yksinkertaisemmat kysymykset olisi ollut tehokkaampia. Tämän vuoksi oli hyvä, että olimme itse henkilökohtaisesti haastattelemassa henkilöitä. Näin saimme paljon lisää tietoa käytännöistä ja mielipiteistä. Haastattelemiemme henkilöiden kanssa saimme sovittua hyvin haastatteluajankohdat ja kaikki olivat yhteistyöhaluisia. Kyselylomakkeiden ja haastatteluiden purkaminen oli työläs vaihe opinnäytetyössämme, vaikka se sujui ilman suurempia ongelmia. Saimme hyvin selvitettyä niistä nykytilan, jonka pohjalta aloimme miettiä itse ohjeistusta.

Kirjallisuutta ja tietoa etsimme tietoturvallisuudesta koko työmme ajan. Tietoturvasta kirjallisuutta löytyi paljon, mutta se ei aina ollut tuoretta. Ajankohtaisen kirjallisuuden löytäminen oli vaikeaa, koska uusimpia kirjoja oli vaikea saada kirjastosta. Hyvää ajankohtaista tietoa löytyi hyvin myös lehtiartikkeleista ja Internetistä.

Tietoturvaohjeistuksesta tuli yleinen, koska ainakaan tässä vaiheessa myymälä- ja varastohenkilökunnalla ei ole tietoturvavastuuta yrityksessä. Tämän hetken tietämys asioista oli suhteellisen vähäinen, mielestämme henkilökunnalle pitäisi järjestää koulutusta tietoturvallisuudesta. Ohjeistuksemme toimii nykyisessä tilanteessa, mutta tarkempia ohjeita saatetaan tarvita jatkossa. Ohjeemme osoittavat myös atk-osastolle, mihin seikkoihin henkilökunnan kanssa tulisi paneutua.

Opinnäytetyömme tavoitteena oli tehdä tietoturvaohjeistus toimeksiantajallemme Vapaa Valinnalle sekä kartoittaa myymälöiden tietoturvan nykytila. Mielestämme pääsimme hyvin tavoitteeseen. Työn tekemisessä kesti yllättävän kauan. Työ valmistui pari kuukautta myöhemmin, mitä olimme ajatelleet.

Tietoturva tulee lähitulevaisuudessa muuttumaan ja kehittymään nopeasti, siksi yritysten tulisi panostaa tietoturvallisuuteen ja pysytellä asioissa ajan tasalla. Tällä hetkellä tietoturvallisuuden yksi tärkeimmistä edellytyksistä on ohjelmistojen päivittäminen.

Lähteet

Hirsjärvi, S. Remes, P. & Sajavaara, P. 2000. Tutki ja kirjoita. Helsinki: Tammi.

Järvinen, P. 2006. Paranna tietoturvaasi. Porvoo. WS Bookwell.

Järvinen, P. 2002. Tietoturva & yksityisyys. Porvoo. WS Bookwell.

Koskivirta, P. 2006. Näin motivoit henkilöstön käyttäytymään tietoturvallisesti. Turvallisuus 3, 14-17.

Kotilainen, L. 2006. Analyysi antaa kuvan yrityksen kokonaistietoturvasta. Turvallisuus 4, 24-25.

Paavilainen, J. 2004. Tietoturvallisuuden perusteet. [online][viitattu 23.11.2006] www.cs.uta.fi/titu/luennot/11_luento_riskienhallinta.pdf

Valtiovarainministeriö 2003. Käyttäjän tietoturvaohje 5/2003. [online][viitattu 28.11.2006] www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/51027/51024_fi.pdf

Yrityksen tietoturvaopas 2006. [online][viitattu 11.09.2006]. www.tietoturvaopas.fi/yrityksen_tietoturvaopas/pdf/Tietoturvaohjeet.pdf

Yrityksen tietoturvaopas 2006. [online][viitattu 11.09.2006]. www.tietoturvaopas.fi/yrityksen_tietoturvaopas/selkeat_ohjeet_tarvitaan.html

Liite 1

Tietoturvaohjeistus

Hallinnollinen tietoturva

- Myymälöiden ja varaston tietoturvapolitiikan tulee määritellä yrityksen johdon tai atk-osaston
- Ohjeistukset myymälöihin ja varastolle johdolta tai atk-osastolta

Fyysinen turvallisuus

- Määriteltävä normaalit ja poikkeusreitit myymälöiden ja varaston tiloihin
- Hätäuloskäynnit tulee olla merkittynä selkeästi
- Murto-, varashälyttimien ja paloilmoitinjärjestelmän toiminta tarkistettava/testattava säännöllisesti
- Vierailijoilta/edustajilta varmistettava henkilöllisyys
- Vierailijaa ei jätetä yksin henkilökunnan tiloihin

Laitteistoturvallisuus

- Tietokone lukittava siltä poistuttaessa, varsinkin jos myymälän tietokone on myymälätiloissa eikä lukitussa tilassa
- Kassakone lukittava aina siltä poistuttaessa
- Salasanoja vaihdettava säännöllisin väliajoin sekä myymälän tietokoneelle että kassakoneille
- Henkilökunnan oikeudet tietokoneille tulisi määritellä tehtävien mukaan
- Laitteen rikkoutuessa ilmoitettava vastuuhenkilölle
- Koulutukset poikkeustilanteita varten, esim. sähkökatkoksien varalta

Ohjelmistoturvallisuus

- Tietoa haittaohjelmista henkilökunnalle
- Henkilökunnalle yleistietoa viruksentorjunnasta ja viruksentorjuntaohjelmasta
- Ohjelmistoihin, kuten Merx-toiminnanohjausjärjestelmään, vaihdettava salasanoja säännöllisin väliajoin
- Merx-toiminnanohjausjärjestelmään ja raportointi-ohjelmaan tulisi määritellä rajattu käyttöoikeus henkilökunnan tehtävien mukaan
- Merx-toiminnanohjausjärjestelmään tulisi olla jokaisella käyttäjällä oma käyttäjätunnus ja salasana, jotta käyttäjä pystyttäisiin tunnistamaan
- Vapaa Valinnan nettisivut suojattava ulkopuolisilta

Tietoaineistoturvallisuus

- Tietoja tulisi käsitellä Vapaa Valinnan yhtenäisten ohjeiden mukaan. Kaikilla myymälöillä ja varastolla tulisi olla yhtenäiset ohjeet koskien tietojen säilytystä, siirtoa, kopiointia, hävittämistä ja jakelua.
- Ohjeistukset tulisi päivittää säännöllisesti
- Poistuttaessa edes hetkeksi kassapäätteeltä tai tietokoneelta on se lukittava
- Kassoilla ja muualla myymälässä luottamukselliset aineistot tulisi säilyttää lukkojen takana

Käyttöturvallisuus

- Työntekijällä tulisi olla varahenkilö, joka osaa tarvittaessa hänen työnsä
- Myymälöissä ja varastolla tulisi olla vähintään kaksi henkilöä, jotka on perehdytetty tarkemmin Vapaa Valinnan tietoturva-asioihin
- Myymälöissä tulisi olla vähintään kaksi henkilöä, jotka on perehdytetty Vapaa Valinnan kassajärjestelmään perusteellisesti ja kassojen tietoturva-asioihin
- Myymälässä ja varastolla tulee olla vähintään kaksi henkilöä, jotka pystyvät neuvomaan Merx-toiminnanohjausjärjestelmän käytössä
- Sähköpostiin oma käyttäjätunnus ja salasana

Tietoliikenneturvallisuus

- Haittaohjelmasta, viruksesta tai virusepäilystä ilmoitus atk-osastolle välittömästi
- Internetiä käytetään ensisijaisesti työtehtävien hoitamiseen, tauolla yksityisasioiden hoitaminen sallittua (jos Internetin käyttö mahdollistetaan myymälöissä ja varastolla)

Henkilöstöturvallisuus

- Henkilökunnan vastuut tulisi määritellä tasaisesti
- Henkilökunnan säännöllinen kouluttaminen tarvekartoituksen mukaan
- Henkilökunnalle tulisi järjestää säännöllisin väliajoin tietoturvallisuuskoulutusta ja -valmennusta
- Vapaa Valinnan uusi työntekijä allekirjoittaa aina työsopimuksen
- Uuden työntekijän tai työharjoittelijan työhön perehdyttämisen yhteydessä kerrotaan Vapaa Valinnan tietoturvaan liittyvät säännöt ja määräykset
- Uuden työntekijän taustatiedot tulisi aina tarkistaa
- Perustettava käyttäjätunnukset ja salasanat uudelle työntekijälle ennen ensimmäistä työpäivää
- Työsuhteen päätyttyä täytyy Vapaa Valinnassa tehdä seuraavia toimenpiteitä:
    - Työntekijälle annetut käyttöoikeudet poistetaan järjestelmistä viimeistään viimeisenä työpäivänä

- Viimeisenä työpäivänä työntekijältä poistetaan kulkuoikeudet
- Ennen lähtöään työntekijän palautettava kaikki Vapaa Valinnan avaimet
- Pois lähtevän työntekijän työtehtävät tulee siirtää asianmukaisesti muille työntekijöille ja muistaa tiedottaa asiasta kaikille asianosaisille

Liite 2

Kyselylomake

1. Fyysinen turvallisuus

Fyysinen turvallisuus on sekä rakenteellista turvallisuutta, kuten ovet ja lukot, että rikostorjuntaan liittyvää turvallisuutta, kuten kamera-valvonta. Fyysinen turvallisuus tulee huomioida jo rakennuksen suunnitteluvaiheessa.

1. miten kulunvalvonta on suoritettu yrityksessä?

_____

_____

2. ovatko yrityksen ulko-ovet ja ikkunat lukittuna?

   Kyllä ☐ Ei ☐ En tiedä ☐

3. onko toimitiloissa hälytysjärjestelmä, esim. murron varalta?

   Kyllä ☐ Ei ☐ En tiedä ☐

4. onko toimitiloissa paloilmoitinjärjestelmä?

   Kyllä ☐ Ei ☐ En tiedä ☐

5. onko toimitiloissa sammutusjärjestelmä?

   Kyllä ☐ Ei ☐ En tiedä ☐

6. miten vieraat vastaanotetaan ja miten he saavat liikkua?

_____

_____

7. onko käytössä vieraiden seurantalistaa?

   Kyllä ☐ Ei ☐ En tiedä ☐

8. onko lähiverkon palvelimet sijoitettu lukittuihin tiloihin, joihin on pääsy vain nimetyillä henkilöillä?

   Kyllä ☐ Ei ☐ En tiedä ☐

9. onko kaikilla omat salasanat ja käyttäjätunnukset tietokoneille?

   Kyllä ☐ Ei ☐ En tiedä ☐

10. kuinka usein salasana vaihdetaan?

2. Laitteistoturvallisuus

Laitteistoturvallisuus tarkoittaa, että laitteet on inventoitu, niiden sijainnista ja kokoonpanosta ollaan selvillä ja niiden varaosien saanti sekä kriittiset järjestelmät on turvattu. Tämä voi käsittää esimerkiksi laitteiden kahdentamisen ja energian saannin varmistamisen sekä huoltosopimuksista huolehtimisen.

1. onko laitteistoihin pääsy toteutettu ainakin käyttäjätunnuksella ja salasanalla?

   Kyllä ☐ Ei ☐ En tiedä ☐

2. vaihdetaanko salasanat tietyin väliajoin?

   Kyllä ☐ Ei ☐ En tiedä ☐

3. pystyvätkö muut kuin järjestelmän hoitaja muuttamaan toisten tietoja ja tiedostoja?

   Kyllä ☐ Ei ☐ En tiedä ☐

4. voivatko tiedot joutua ulkopuolisille?

   Kyllä ☐ Ei ☐ En tiedä ☐

5. onko tietokoneiden väärinkäyttö estetty esim. BIOS-, virta-, näppäimistö- tai näytönsäästäjäsalasanoilla?

   Kyllä ☐ Ei ☐ En tiedä ☐

6. pystytäänkö laitteistovian sattuessa kyseinen laite korvaamaan nopeasti?

   Kyllä ☐ Ei ☐ En tiedä ☐

7. saavatko tärkeimmät laitteet energiaa, esim. sähkökatkon aikana?

   Kyllä ☐ Ei ☐ En tiedä ☐

3. Ohjelmistoturvallisuus

Ohjelmistoturvallisuuteen voidaan organisaatiossa vaikuttaa määrittelemällä, mitkä ohjelmistot ovat sallittuja tai ainakin mitä ei missään tapauksessa sallita käytettäväksi.

1. onko joka laitteella viruksentorjuntaohjelma?

   Kyllä ☐ Ei ☐ En tiedä ☐

2. millainen viruksentorjunta ohjeistus yrityksellä on?

_____

_____

3. osaako koko henkilökunta toimia oikein viruksen yllättäessä?

   Kyllä ☐ Ei ☐ En tiedä ☐

4. miten usein virustarkistus tehdään?

_____

_____

5. onko yrityksen koneille joskus päässyt virus?

   Kyllä ☐ Ei ☐ En tiedä ☐

   Miten?

_____

_____

_____

6. kirjataanko suojattuun lokitiedostoon tärkeimpien ohjelmistojen tapahtumatiedot?

   Kyllä ☐ Ei ☐ En tiedä ☐

7. onko nettisivut suojattu niin, että niitä ei pysty ulkopuoliset muuttamaan?

   Kyllä ☐ Ei ☐ En tiedä ☐

8. käytetäänkö tietokoneissa tiedostojen salaamista?

   Kyllä ☐ Ei ☐ En tiedä ☐

9. onko yrityksen käyttämät ohjelmistot lisensoitu?

   Kyllä ☐ Ei ☐ En tiedä ☐

10. onko kaikista hankituista ohjelmistoista käsikirjat ja lähdekoodi?

    Kyllä ☐ Ei ☐ En tiedä ☐

11. onko lisenssiluettelo tehty/tallessa?

    Kyllä ☐ Ei ☐ En tiedä ☐

12. onko ohjelmisto CD:t varmassa tallessa?

    Kyllä ☐ Ei ☐ En tiedä ☐

4. Tietoaineistoturvallisuus

Tietoaineistoturvallisuuteen liittyvät myös tiedon jatkuva varmistaminen, asianmukainen säilytys sekä hävittäminen. Tietoaineistoturvallisuudella pyritään säilyttämään asiakirjojen, tietueiden ja tiedostojen luottamuksellisuus sekä estämään tietojen tuhoutuminen tai tahaton muuttuminen. Oleellista on myös tallenteiden suojaaminen ja oikeanlainen säilyttäminen.

1. millaiset säännöt yrityksellä on tietojen säilytyksestä?

   _____

   _____

2. millaiset säännöt yrityksellä on tietojen kuljetuksesta?

3. millaiset säännöt yrityksellä on tietojen kopioinnista?

4. millaiset säännöt yrityksellä on tietojen hävittämisestä?

5. millaiset säännöt yrityksellä on tietojen jakelusta?

6. millaiset säännöt yrityksellä on tietojen käytöstä normaali- ja katastrofitilanteissa?

7. Onko yrityksellä käytössä tietojen luokitusjärjestelmä?

   Kyllä ☐ Ei ☐ En tiedä ☐

   Millainen?

8. miten luku-, kirjoitus- ja muutosoikeudet on jaoteltu työntekijöiden kesken?

9. millaiset yhteiset tietovarastot on käytettävissä, esim. tuotetietokannat?

10. kuinka tietovarastoille on annettu käyttöoikeuksia?

    Kyllä ☐ Ei ☐ En tiedä ☐

11. onko työntekijöillä rajattu pääsy vain omiin työtehtävän edellyttämiin tietoihin?

    Kyllä ☐ Ei ☐ En tiedä ☐

12. minkälaisille tallenteille yrityksen tietoja tallennetaan, esim. CD-ROM, paperi, levyke, mikrofilmi, jne.?

13. onko luottamuksellisia ja salaisia tietoja sisältävä tietokantapalvelin yhteydessä internetiin?

    Kyllä ☐ Ei ☐ En tiedä ☐

    miten se on suojattu?

14. miten sähköposti on suojattu?

15. miten eri tallenteet hävitetään yrityksessä esim. paperi, levyke, mikrofilmi, jne.?

16. muistetaanko tiedon syntyvaiheessa myös luonnokset hävittää oikein?

    Kyllä ☐ Ei ☐ En tiedä ☐

17. onko huolehdittu tietoliikenteen kautta kulkevien aineistojen salaus?

    Kyllä ☐ Ei ☐ En tiedä ☐

18. ovatko asiakkaan luottamukselliset tiedot turvassa?

    Kyllä ☐ Ei ☐ En tiedä ☐

5. Käyttöturvallisuus

Käyttöturvallisuus koostuu monesta asiasta; järjestelmien turvallisista käyttöperiaatteista, tietojenkäsittelytapahtumien valvonnasta sekä jatkuvuuden turvaamisesta. Periaatteena on luoda sellaiset menettelytavat, joilla päivittäisessä toiminnassa säilytetään tietoturvallisuuden taso mahdollisimman hyvänä.

1. miten työntekijöiden käyttöoikeudet on määritelty?

2. miten varmuuskopiointi on suoritettu?

3. onko työntekijällä varamies, joka tarvittaessa osaa hänen työt?

    Kyllä ☐ Ei ☐ En tiedä ☐

4. jos jokin laite menee rikki, niin kuinka nopeasti se saadaan taas käyttöön/korvattua?

5. onko yrityksellä toipumissuunnitelma erilaisiin poikkeaviin tilanteisiin?

   Kyllä ☐ Ei ☐ En tiedä ☐

6. kuinka usein varmuuskopiointi suoritetaan?

6. Henkilöstöturvallisuus

Henkilöstöturvallisuus käsittää koko henkilöstön liikkumiseen, matkustamiseen ja tunnistamiseen liittyvät seikat, mutta myös yksityisyyden suojaan, taustojen tarkistamiseen, motivaation ylläpitämiseen ja kouluttamiseen.

1. tarkistetaanko uusien työntekijöiden taustatiedot?

   Kyllä ☐ Ei ☐ En tiedä ☐

2. allekirjoittaako jokainen uusi työntekijä vaitiolosopimuksen?

   Kyllä ☐ Ei ☐ En tiedä ☐

3. huolehditaanko työsuhteen päättyessä kyseisen henkilön käyttöoikeuksien, kulkulupien yms. poistamisesta?

   Kyllä ☐ Ei ☐ En tiedä ☐

4. onko avainhenkilöille nimetty varahenkilöt?

   Kyllä ☐ Ei ☐ En tiedä ☐

5. onko työt jaettu henkilökunnan kesken niin, että yhdelle henkilölle ei kasautuisi liikaa vastuita?

   Kyllä ☐ Ei ☐ En tiedä ☐

6. miten tietoturvallisuuteen liittyvät vastuut ja velvollisuudet on määritelty toimenkuvassa?

7. koulutetaanko henkilökuntaa poikkeustilanteita varten?

   Kyllä ☐ Ei ☐ En tiedä ☐

   Miten?

7. Hallinnollinen tietoturva

Hallinnollinen tietoturva koostuu johdon hyväksymistä periaatteista, vastuunjaosta, tarkoitukseen varatuista resursseista sekä riskien arvioinnista.

1. millainen yrityksen tietoturvapolitiikka on?

2. onko yrityksellä toipumissuunnitelma katastrofin varalle?

   Kyllä ☐ Ei ☐ En tiedä ☐

   Millainen?

3. mitä suojattavia kohteita yrityksellä on, esim. verkko, laitteet, tietokannat, järjestelmät jne.? miten ne on suojattu?

4. onko yritys joutunut yritysvakoilun kohteeksi?

   Kyllä ☐ Ei ☐ En tiedä ☐

5. onko tietoturva vastuut määritelty?

   Kyllä ☐ Ei ☐ En tiedä ☐

6. onko henkilökunnalle kerrottu mitkä asiat on salassa pidettäviä?

   Kyllä ☐ Ei ☐ En tiedä ☐

7. millainen tietoturvaohjeistus yrityksellä on?

_____

_____

_____

8. onko mietitty vastuukysymyksiä asiakkaiden osalta mahdollisen vahingon sattuessa?

   Kyllä ☐ Ei ☐ En tiedä ☐

8. Tietoliikenneturvallisuus

Tietoliikenneturvallisuus tarkoittaa siirrettävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaamista tietojen siirron aikana. Tähän osa-alueeseen kuuluu mm. salaus, verkon palveluvarmuuden turvaaminen, turvallisen reitityksen järjestäminen, vain sallittujen palveluiden salliminen, vaihtoehtoisten tiedonsiirtotapojen suunnittelu, yksityisyyden suoja yms.

1. onko tietoliikennekapasiteettia turhaan kuormitettuna?

   Kyllä ☐ Ei ☐ En tiedä ☐

2. onko varauduttu käyttämään vaihtoehtoisia tiedonsiirtotapoja?

   Kyllä ☐ Ei ☐ En tiedä ☐

3. onko kaikki tietoliikenneyhteydet suojattu?

   Kyllä ☐ Ei ☐ En tiedä ☐

   Miten?

4. onko turhat palvelut karsittu palvelimelta?

   Kyllä ☐ Ei ☐ En tiedä ☐

5. onko www-palvelin sijoitettu erilliseen, suojattuun aliverkkoon?

   Kyllä ☐ Ei ☐ En tiedä ☐

6. miten hakkerointiin on varauduttu?

7. pääseekö työntekijä toisen työntekijän tiedostoihin, esim. netin kautta?

   Kyllä ☐ Ei ☐ En tiedä ☐

8. ovatko tietoliikenteellä varmistukset/vaihtoehtoiset reitit katkon sattuessa?

   Kyllä ☐ Ei ☐ En tiedä ☐